



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

52

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/833,922	04/12/2001	Gregory O'Shea	208797	3840

23460 7590 03/18/2005

LEYDIG VOIT & MAYER, LTD
TWO PRUDENTIAL PLAZA, SUITE 4900
180 NORTH STETSON AVENUE
CHICAGO, IL 60601-6780

EXAMINER

PARTHASARATHY, PRAMILA

ART UNIT	PAPER NUMBER
----------	--------------

2136

DATE MAILED: 03/18/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary

Application No.

09/833,922

Applicant(s)

O'SHEA ET AL.

Examiner

Pramila Parthasarathy

Art Unit

2136

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 18 January 2005.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1,2,5-13 and 16-25 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1,2,5-13 and 16-25 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. _____.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____
- 4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____
- 5) ☐ Notice of Informal Patent Application (PTO-152)
- 6) ☐ Other: _____

DETAILED ACTION

1. This action is in response to request for reconsideration filed on January 18, 2005. Claims 3, 4, 14 and 15 were cancelled. Claims 1, 2, 5, 6, 8, 9, 12, 13 and 16 were amended. No new Claims were added. Therefore, presently pending claims are 1, 2, 5 – 13 and 16 – 25.

Response to Arguments

2. Applicant's arguments filed on January 18, 2005, have been fully considered but they are not persuasive for the following reasons:

3. Applicant argued that the cited prior art (CPA) [Diffie (U.S. Patent number RE.36,946, hereafter "Diffie")] does not teach, suggest or disclose "the network address of the mobile computing device ... having a portion derived from the public key of the mobile computing device", "data for updating a care-of address of the mobile computing device".

4. Diffie teaches a method for providing a secure communication between two devices by sending a digital signature, which contains a binding between the public key and machine name (network address) that is digitally signed using a private key and both parties exchange certificates for future data transfer (Column 1 line 49 – Column 2

line 20; Column 7 lines 6 – 10 and Column 10 lines 14 – 35). Diffie also teaches that both the devices verify all messages (digital signature with public key information of the both device) and authenticate before processing or before entering data transfer phase (Column 8 lines 7 – 64 and Column 10 lines 41 – 45). Diffie further teaches the content data include data for updating a care-of address of a computing device (Column 5 line 34 – Column 6 line 18 and Column 8 lines 18 – 64), wherein the content data include public key of the base, digital signature (binding between the public key and the machine name (care-of address)) of a computing device.

5. Regarding Claims 1, 12 and 13, Diffie teaches and describes a method for a mobile computing device to make authentication information (message) including public key of the mobile computing device, a digital signature, a binding between the public key and a logical identifier of the machine (network address) having a portion derived from the public key of the mobile computing device (Column 1 line 49 – Column 2 line 20 and Column 8 lines 7 – 23 and 41 – 48). Diffie also teaches that the message will include public key of the mobile and base device along with logical identifier of the machine (network address) wherein the certificate is digitally signed by the private key of the first device (Column 8 lines 49 – 67).

Diffie further teaches that the content data include data for updating a care-of address of a computing device (Column 5 line 34 – Column 6 line 18 and Column 8 lines 18 – 64), wherein the content data include data for updating a public key of the device (digital signature with the public key and the machine name (care-of address)).

6. Regarding Claims 20 and 25, Diffie teaches and describes a method for a first computing device to make authentication information (message) including public key of the first computing device computing device to make authentication information (message) including public key of the first computing device, a digital signature, a binding between the public key and a logical identifier of the machine (network address) deriving a portion of a second network address from the public key of the first computing device (Column 1 line 49 – Column 2 line 20 and Column 8 lines 7 – 23 and 41 – 48). Diffie also teaches that the both device receive other device's message containing digitally signed digital signature (network address) and decrypts the authenticated message to drive the network address of the other device (Column 1 line 49 – Column 2 line 14 and Column 8 lines 41 – 67).

7. Applicant clearly has failed to explicitly identify specific claim limitations, which would define a patentable distinction over prior arts. Therefore, the examiner respectfully asserts that CPA does teach or suggest the subject matter broadly recited in independent claims 1, 12, 13, 20 and 25. Dependent claims 2, 5 – 13, 16 – 19 and 21 – 24 are also rejected at least by virtue of their dependency on independent claims and by other reason set forth in this and previous (September 14, 2004) office action. Accordingly, the rejection for the pending Claims 1, 2, 5 – 13 and 16 – 25 is respectfully maintained.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in a patent granted on an application for patent by another filed in the United States before the invention thereof by the applicant for patent, or on an international application by another who has fulfilled the requirements of paragraphs (1), (2), and (4) of section 371(c) of this title before the invention thereof by the applicant for patent.

8. Claims 1, 2, 5 – 13 and 16 – 25 are rejected under 35 U.S.C. 102(e) as being anticipated by Diffie et al (U.S. Patent Number Re. 36,946).

9. Regarding Claim 1, Diffie teaches and describes a method for a mobile computing device to make authentication information available to a base computing device (Fig. 2, 3, 4a – 4c, 5a, 5b; and Column 4 line 6 – Column 10 line 53), the method comprising:

creating authentication information, the authentication information including content data that include data for updating a care-of address of the mobile computing device (Column 5 line 34 – Column 6 line 18 and Column 8 lines 18 – 64),

Diffie teaches that the content data include data for updating a public key of the device (digital signature with the public key and the machine name (care-of address)),

a public key of the first computing device, a network address of the mobile computing device, and a digital signature, the network address having a portion derived from the public key of the mobile computing device, the digital signature generated by

signing with a private key of the mobile computing device corresponding to the public key, the digital signature generated from data in the set: the content data, a hash value of data including the content data (Fig. 4a – 4c, 5a; and Column 1 line 49 – Column 2 line 20 and Column 7 lines 6 – 45); and

making the authentication information available to the second computing device.

10. Regarding Claim 12, Diffie teaches and describes a computer-readable medium containing instructions for performing a method for a first computing device to make authentication information available to a second computing device (Fig. 2, 3, 4a – 4c, 5a, 5b; and Column 4 line 6 – Column 10 line 53), the method comprising:

creating authentication information, the authentication information including content data that include data for updating a care-of address of the first computing device (Column 5 line 34 – Column 6 line 18 and Column 8 lines 18 – 64),

Diffie teaches that the content data include data for updating a public key of the device (digital signature with the public key and the machine name (care-of address)),

a public key of the first computing device, a network address of the first computing device, and a digital signature, the network address having a portion derived from the public key of the first computing device, the digital signature generated by signing with a private key of the first computing device corresponding to the public key, the digital signature generated from data in the set: the content data, a hash value of data including the content data (Fig. 4a – 4c, 5a; and Column 1 line 49 – Column 2 line 20 and Column 7 lines 6 – 45);

making the authentication information available to the second computing device.

11. Regarding Claim 13, Diffie teaches and describes a computer-readable medium having stored thereon a data structure (Fig. 2, 3, 4a – 4c, 5a, 5b; and Column 4 line 6 – Column 10 line 53), the data structure comprising:

content data that include data for updating a care-of address of a computing device (Column 5 line 34 – Column 6 line 18 and Column 8 lines 18 – 64),

Diffie teaches that the content data include data for updating a public key of the device (digital signature with the public key and the machine name (care-of address)),

a public key of the computing device; a network address of the computing device, the network address having a portion derived from the public key of the computing device; and a digital signature, the digital signature generated by signing with a private key of the computing device corresponding to the public key, the digital signature generated from data in the set: the content data, a hash value of data including the content data (Fig. 4a – 4c, 5a; and Column 1 line 49 – Column 2 line 20 and Column 7 lines 6 – 45).

12. Regarding Claim 20, Diffie teaches and describes 20. A method for a second computing device to authenticate content data made available by a first computing device (Fig. 2, 3, 4a – 4c, 5a, 5b; and Column 4 line 6 – Column 10 line 53), the method comprising;

accessing authentication information made available by the first computing

device, the authentication information including the content data, a public key of the first computing device, a first network address of the first computing device, and a digital signature; deriving a portion of a second network address from the public key of the first computing device; validating the digital signature by using the public key of the first computing device; accepting the content data if the derived portion of the second network address matches a corresponding portion of the first network address and if the validating shows that the digital signature was generated from data in the set: the content data, a hash value of data including the content data (Fig. 4a – 4c, 5a, 5b; and Column 1 line 49 – Column 2 line 20 and Column 7 line 46 – Column 8 line 58).

13. Regarding Claim 25, Diffie teaches and describes 25. A computer-readable medium containing instructions for performing a method for a second computing device to authenticate content data made available by a first computing device (Fig. 2, 3, 4a – 4c, 5a, 5b; and Column 4 line 6 – Column 10 line 53), the method comprising:

accessing authentication information made available by the first computing device, the authentication information including the content data, a public key of the first computing device, a first network address of the first computing device, and a digital signature; deriving a portion of a second network address from the public key of the first computing device; validating the digital signature by using the public key of the first computing device; accepting the content data if the derived portion of the second network address matches a corresponding portion of the first network address and if the validating shows that the digital signature was generated from data in the set: the

content data a hash value of data including the content data (Fig. 4a – 4c, 5a, 5b; and Column 1 line 49 – Column 2 line 20 and Column 7 line 46 – Column 8 line 58).

14. Claim 2 is rejected as applied about in rejecting Claim 1. Furthermore, Diffie discloses a method for a mobile computing device to make authentication information available to a base computing device (Fig. 2, 3, 4a – 4c, 5a, 5b; and Column 4 line 6 – Column 10 line 53), wherein the authentication information is made available to the base computing device by sending a message incorporating the authentication information to the base computing device (Column 7 lines 38 – 45).

15. Claims 5 and 16 are rejected as applied about in rejecting Claim 1 and 13. Furthermore, Diffie discloses a method for a mobile computing device to make authentication information available to a second computing device (Fig. 2, 3, 4a – 4c, 5a, 5b; and Column 4 line 6 – Column 10 line 53), wherein the second computing device is a home agent for the mobile computing device, and wherein the network address of the mobile computing device is a home address of the mobile computing device (Column 7 lines 6 – 10).

16. Claim 6 is rejected as applied about in rejecting Claim 1. Furthermore, Diffie discloses a method for a mobile computing device to make authentication information available to a base computing device (Fig. 2, 3, 4a – 4c, 5a, 5b; and Column 4 line 6 – Column 10 line 53), wherein the base computing device is a correspondent of the

mobile computing device, and wherein the network address of the mobile computing device is a home address of the mobile computing device (Column 7 lines 6 – 10).

17. Claim 7 is rejected as applied about in rejecting Claim 1. Furthermore, Diffie discloses a method for a mobile computing device to make authentication information available to a base computing device (Fig. 2, 3, 4a – 4c, 5a, 5b; and Column 4 line 6 – Column 10 line 53), wherein the public key and the private key together form an uncertified key pair (Column 5 line 51 – Column 6 line 7).

18. Claims 8 and 17 are rejected as applied about in rejecting Claims 1 and 13. Furthermore, Diffie discloses a method for a mobile computing device to make authentication information available to a base computing device (Fig. 2, 3, 4a – 4c, 5a, 5b; and Column 4 line 6 – Column 10 line 53), wherein the network address of the mobile computing device includes a route prefix portion and a node-selectable portion, and the node-selectable portion includes a portion of a hash value of data including the public key of the mobile computing device (Column 7 lines 6 – 29).

19. Claims 10 and 19 are rejected as applied about in rejecting Claims 1 and 13. Furthermore, Diffie discloses a method for a mobile computing device to make authentication information available to a base computing device (Fig. 2, 3, 4a – 4c, 5a, 5b; and Column 4 line 6 – Column 10 line 53), wherein the authentication information further includes data for preventing a replay attack (Column 8 lines 12 – 58).

20. Claim 21 is rejected as applied about in rejecting Claim 20. Furthermore, Diffie discloses a method for a first computing device to make authentication information available to a second computing device (Fig. 2, 3, 4a – 4c, 5a, 5b; and Column 4 line 6 – Column 10 line 53), further comprising:

determining whether to accept the content data based on a time stamp in the authentication information (Column 7 lines 6 – 10 and Column 8 lines 18 – 32).

21. Claims 9 and 18 are rejected as applied about in rejecting Claims 8 and 17. Furthermore, Diffie discloses a method for a mobile computing device to make authentication information available to a base computing device (Fig. 2, 3, 4a – 4c, 5a, 5b; and Column 4 line 6 – Column 10 line 53), wherein the node-selectable portion includes a portion of a hash value of data including the public key of the mobile computing device and a modifier selected for preventing address conflicts (Column 7 lines 23 – 45).

22. Claim 11 is rejected as applied about in rejecting Claim 10. Furthermore, Diffie discloses a method for a first computing device to make authentication information available to a second computing device (Fig. 2, 3, 4a – 4c, 5a, 5b; and Column 4 line 6 – Column 10 line 53), wherein the data for preventing a replay attack are in the set: time stamp, data identifying the second computing device as an intended recipient of the authentication information (Column 7 lines 6 – 45 and Column 8 lines 49 – 58).

23. Claim 22 is rejected as applied about in rejecting Claim 20. Furthermore, Diffie discloses a method for a first computing device to make authentication information available to a second computing device (Fig. 2, 3, 4a – 4c, 5a, 5b; and Column 4 line 6 – Column 10 line 53), wherein the content data include data for updating a communications parameter for the first computing device, the method further comprising:

updating a record of a communications parameter for the first computing device (Column 7 line 38 – Column 8 line 67).

24. Claim 24 is rejected as applied about in rejecting Claim 20. Furthermore, Diffie discloses a method for a first computing device to make authentication information available to a second computing device (Fig. 2, 3, 4a – 4c, 5a, 5b; and Column 4 line 6 – Column 10 line 53), wherein the authentication information further includes a modifier, and wherein deriving includes appending the modifier to the public key of the first computing device before deriving a portion of the second network address (Column 8 lines 7 – 68).

25. Claim 23 is rejected as applied about in rejecting Claim 22. Furthermore, Diffie discloses a method for a first computing device to make authentication information available to a second computing device (Fig. 2, 3, 4a – 4c, 5a, 5b; and Column 4 line 6 – Column 10 line 53), wherein the communications parameter is a care-of address of

Art Unit: 2136

the first computing device, and wherein updating includes updating a routing table maintained by the second computing device (Column 8 lines 7 – 68).

Conclusion

26. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. See PTO Form 892.

27. THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Pramila Parthasarathy whose telephone number is 571-272-3866. The examiner can normally be reached on 8:00a.m. To 5:00p.m..

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 571-232-3795.


Art Unit: 2136

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 703-305-3900.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR only. For more information about the PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Pramila Parthasarathy

March 13, 2005.


AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100